Publicado en *Security In A Box* (https://securityinabox.org)

11. Utilizar los teléfonos inteligentes de la manera más segura posible

En el ***Capítulo 10: Utilizar los teléfonos móviles de la manera más segura posible*** [1], conversamos sobre los retos de la seguridad al usar teléfonos móviles convencionales – incluidos los temas sobre los servicios de comunicación por voz y mensajes de textos (SMS/MSS). Estos teléfonos móviles primordialmente (sino exclusivamente) utilizan redes móviles para transferir llamadas y datos.

Actualmente, los avances tecnológicos han posibilitado que los teléfonos móviles contengan servicios y características similares a las computadoras de escritorio o portátiles. Estos teléfonos inteligentes ofrecen nuevas y variadas formas para comunicarse, capturar y difundir medios de comunicación. Para proveer estas nuevas funcionalidades, los teléfonos inteligentes no sólo utilizan la red móvil sino que se conectan a la internet a través de una conexión WiFi (similar a una computadora portátil en un café internet) o a través de un operador de red móvil.

Por lo tanto, aunque puedes realizar llamadas con un teléfono inteligente, es mejor considerar los teléfonos inteligentes como pequeños dispositivos de computación. Esto significa que el otro material didáctico de este kit de herramientas es relevante para el uso de tu teléfono inteligente así como para tu computadora.

Los teléfonos inteligentes usualmente son compatibles con una amplia gama de funcionalidades – navegación en internet, correo electrónico, mensajería de voz y de texto a través de la internet, capturar, guardar y transmitir audios, videos y fotos, habilitar redes sociales, juegos en línea con varios usuarios a la vez, banca en internet, y muchas otras actividades. Sin embargo muchas de estas herramientas y características implican nuevos temas de seguridad, o aumentan riesgos ya existentes.

Por ejemplo, algunos teléfonos inteligentes tienen incorporados una funcionalidad de geo-localización (*GPS* [2]), lo cual significa el teléfono le provee automáticamente al operador de red móvil tu ubicación exacta, como a las aplicaciones que utilizas en tu teléfono inteligente (tales como redes sociales, mapas, navegadores y otras aplicaciones). Como mencionamos anteriormente, el teléfono móvil ya transmite la información de tu ubicación al operador de la red móvil (como funciones normales del teléfono). Sin embargo, la funcionalidad adicional del GPS no sólo incrementa la precisión de la información sobre tu ubicación, sino que además aumenta la cantidad de lugares en las que esta información puede ser distribuida.

Vale la pena revisar todos los riesgos asociados con los teléfonos móviles abordados en el ***Capítulo 10: Utilizar los teléfonos móviles de la manera más segura posible*** [1] ya que también son relevantes para el uso de teléfonos inteligentes. El ***Capítulo 10*** [1] abarca temas sobre escuchas ilegales, interceptación de SMS y/o llamadas teléfonicas, temas sobre las tarjetas SIM, y buenas prácticas.

En este capítulo abordaremos los retos adicionales a la seguridad que trae consigo el uso de los teléfonos inteligentes.

Bolsos, Billeteras, Télefonos Inteligentes

Intuitivamente comprendemos lo importante que es mantener seguros nuestros bolsos y billeteras, ya que sabemos que en ellos guardamos información sensible, y perderlos podría comprometer nuestra privacidad y seguridad. Las personas son menos conscientes de la cantidad de información personal que tienen en sus teléfonos inteligentes, y consideran la pérdida del teléfono más una molestia y no un riesgo. Si consideras al teléfono inteligente como un dispositivo de computación que siempre se encuentra conectado a una red y continuamente es trasladado de un lugar a otro, se destaca la diferencia entre portar información discreta y pasiva como la billetera, y portar un elemento activo e interactivo como un teléfono inteligente.

Un simple ejercicio nos puede ilustrar esto:

Vacía el contenido de tu bolso o billetera, y tome en cuenta los elementos sensibles que contienen. Normalmente encontrarás: - Fotos de las personas que amas (~5 fotos) - Tarjetas de identificación (licencia de conducir, tarjetas de membresía, documento de identidad, etc) - Seguros e información médica (~2 tarjetas) - Dinero (~5 billetes) - Tarjetas de Crédito/Débito (~3 tarjetas)

Ahora examina los contenidos de tu teléfono inteligente. Un usuario típico de teléfono inteligente podría encontrar más cantidad de información que la descrita anteriormente, y en algunos casos muchos más elementos sensibles y valiosos:
- Fotos de las personas que amas (~100 fotos) - Aplicaciones de correo electrónico y sus contraseñas - Correos electrónicos (~500 correos) - Videos (~50 videos) - Aplicaciones de redes sociales y sus contraseñas - Aplicaciones de bancos en internet (con acceso a cuentas bancarias) - Documentos sensibles - Registros sensibles de comunicaciones - Conexión inmediata a tu información sensible

Entre más utilizas los teléfonos inteligentes, debes ser más consciente de los riesgos asociados a ellos y tomar las precauciones necesarias. Los teléfonos inteligentes son potentes amplificadores y distribuidores de tus datos personales. Están diseñados para proporcionar la mayor conectividad posible y acceder automáticamente a los servicios de redes sociales. Esto se debe a que tus datos personales son muy valiosos, y pueden ser agregados, buscados y vendidos.

En el ***Capítulo 5: Recuperar información perdida*** [3] conversamos sobre la importancia de respaldar datos. Esto aplica especialmente para teléfonos inteligentes. Sería un desastre si pierdes tu teléfono sin haber respaldado en un lugar seguro los datos más importantes (tales como tus contactos). Además de respaldar tus datos, asegúrate de conocer cómo recuperar los datos. Guarde una copia impresa de los pasos que debes seguir para que puedas hacerlo rápidamente en caso de emergencia.

En este capítulo iniciaremos con algunos elementos básicos de los teléfonos inteligentes – una descripción de varias plataformas y algunos procedimientos de configuración básicos para la seguridad de tu información y comunicación. Las otras secciones de este capítulo las dedicaremos a cubrir las precauciones específicas relacionadas con los usuarios comunes de teléfonos inteligentes. Secciones posteriores abordarán aspectos de seguridad sobre:

Plataformas, Configuración básica e Instalación

Plataformas y Sistemas Operativos

Al momento de escribir este capítulo, los teléfonos inteligentes de uso más común son el iPhone de Apple y Android de Google, seguidos por el Blackberry y teléfonos de Windows. La mayor diferencia entre el Android y los otros sistemas operativos, es que Android es un sistema, principalmente de Código Abierto (*FOSS* [4]), permitiendo que su sistema operativo sea auditado de forma independiente para verificar si protege apropiadamente la información y comunicación de los usuarios. También facilita el desarrollo de aplicaciones de seguridad para su plataforma. Muchos programadores conscientes de la seguridad desarrollan aplicaciones para Android pensando siempre en la seguridad del usuario. Algunas de estas aplicaciones las destacaremos más adelante en este capítulo.

Sin importar el tipo de teléfono inteligente que utilizas, es importante que seas consciente de algunos temas al usar un teléfono que se conecta a internet y que contiene características tales como *GPS* [5] o capacidad de red inalámbrica. En este capítulo nos enfocamos en dispositivos con la plataforma Android, ya que, como explicamos anteriormente, es más fácil asegurar datos y comunicaciones. Sin embargo, las guías de configuración básicas y algunas aplicaciones para dispositivos que no sean teléfonos Android se proporcionan también.

Los teléfonos Blackberry han sido presentados como dispositivos “seguros” para mensajería y correo electrónico. Esto porque los mensajes y correos electrónicos son dirigidos de forma segura por medio de los servidores de Blackberry, fuera del alcance de potenciales intrusos. Desafortunadamente, más y más gobiernos están demandando acceso a estas comunicaciones, citando la necesidad de protegerse contra el terrorismo y crimen organizado. La India, Emiratos Árabes Unidos, Arabia Saudita, Indonesia y el Líbano son ejemplos de gobiernos que han analizado el uso de dispositivos Blackberry y han exigido el acceso a los datos del usuario en sus países.

Teléfonos móviles convencionales

Otra categoría de teléfonos móviles son llamados comúnmente 'móviles convencionales' (eje. Nokia 7705 Twist o Samsung Rogue). Recientemente, los móviles convencionales han incrementado sus funcionalidades para incluir algunas contenidas en los teléfonos inteligentes. Pero generalmentes, los sistemas operativos de los móviles convencionales son menos accesibles, y por lo tanto existen limitadas oportunidades para aplicaciones de seguridad o mejoras a las mismas. No abordamos específicamente los móviles convencionales, sin embargo muchas de las medidas expresadas en este capítulo también tienen sentido para los móviles convencionales.

Teléfonos inteligentes de marca y bloqueados

Los teléfonos inteligentes usualmente son vendidos con una marca o bloqueados. Un teléfono inteligente bloqueado significa que el dispositivo sólo puede ser operado con un único proveedor, y el dispositivo sólo funciona con su tarjeta SIM. Los proveedores de redes móviles usualmente le ponen marca a los teléfonos mediante la instalación de su propio

"firmware" o software. También puede que los proveedores deshabiliten algunas funcionalidades o agregar otras. La marca es un medio para que las empresas aumenten sus ingresos mediante la canalización del uso de tu teléfono inteligente, a menudo también la recopilando datos acerca de cómo utilizas el teléfono o habilitando el acceso remoto a tu teléfono inteligente.

Por estas razones, recomendamos comprar teléfonos inteligentes desbloqueados, siempre que puedas. Un teléfono bloqueado incrementa los riesgos debido a que tus datos son canalizados a través de un sólo proveedor, centralizando así el flujo de tu información haciendo imposible cambiar las tarjetas SIM para difundir los datos a través de diferentes proveedores. Si tu teléfono está bloqueado, pregúntale a alguien de confianza cómo desbloquearlo.

Configuración General

Los teléfonos inteligentes tienen muchas opciones de configuración que controlan la seguridad del dispositivo. Es importante prestar atención sobre como se encuentra configurado tu teléfono inteligente. En las guías prácticas que se presentan más adelante, te alertaremos sobre algunas opciones de seguridad del teléfono inteligente que están disponibles pero no están activadas por defecto, así como aquellas opciones que se encuentran activadas por defecto y que vulneran tu teléfono.

Guía Práctica: Empezar con la *Guía de Configuración Básica de Android* [6]

Instalar y actualizar aplicaciones

La forma más común de instalar nuevo software en tu teléfono inteligente es usando el Appstore de iPhone o Google Play store, allí ingresas tu información de usuario, y descargas e instalas la aplicación que deseas. Al iniciar la sesión, estás asociando tu información de cuenta de usuario a la tienda virtual. Los dueños de la tienda virtual mantienen registros del historial de navegación del usuario y sus preferencias de aplicaciones.

Las aplicaciones que ofrecen las tiendas virtuales oficiales son, supuestamente, verificadas por los dueños de las tiendas (Google o Apple), pero en la realidad esto provee poca protección contra lo que puede hacer la aplicación una vez instalada en tu teléfono. Por ejemplo, algunas aplicaciones pueden copiar y enviar tu directorio de contactos luego de ser instaladas en tu teléfono. En el caso de los teléfonos Android, durante el proceso de instalación cada aplicación te solicita permiso sobre lo que puede o no hacer una vez en uso. Deberías prestar mucha atención a los tipos de permisos solicitados, y si estos permisos tienen sentido respecto a la funcionalidad de la aplicación que estás instalando. Por ejemplo, si estás considerando instalar una aplicación para "lectura de noticias" y te das cuenta que te solicita derechos para enviar tus contactos a través de una conexión móvil de datos a terceros, deberías buscar otras aplicaciones más acordes con accesos y derechos.

Las aplicaciones de Android también están disponibles fuera de los canales oficiales de Google. Sólo debes marcar la caja de *Fuentes desconocidos* que se encuentra en *Aplicaciones* para poder utilizar estos sitios web de descargas.

Son muy útiles estos sitios web alternativos si quieres minimizar tu contacto en línea con Google. Recomendamos **F-Droid** [7] ('Free Droid'), que sólo ofrece aplicaciones de *FOSS* [8]. En esta guía, F-Droid es el repositorio primordial de las aplicaciones que recomendamos, y

sólo te referimos a Google Play si una aplicación no está disponible en F-Droid.

Si no deseas (o no puedes) conectarte a internet para acceder a las aplicaciones, puedes transferir aplicaciones al teléfono de otra persona enviando archivos ***.apk*** [9] (siglas del inglés para 'paquetes de aplicaciones para android') vía bluetooth. Como alternativa también puedes descargar el archivo .apk a la tarjeta Micro SD de tu dispositivo móvil o utilizar un cable usb para trasladarlo desde una computadora. Cuando hayas recibido el archivo, simplemente haz un pulso largo al archivo y estará listo para instalarse. (**Nota**: sea especialmente cuidadoso/a mientras usas bluetooth – leer más en ***Capítulo 10.2.4: Funciones más allá de la conversación y los mensajes*** [10]).

Comunicándote (Voz y Mensajes) vía Teléfono Inteligente

Conversaciones Seguras

Telefonía Básica

En el capítulo ***10.2.2 Funciones básicas, capacidad de rastreo y anonimato*** [11] conversamos sobre las diferentes medidas que deberías considerar para aminorar los riesgos de interceptación al utilizar los operadores de redes móviles para la comunicación de voz.

Utilizar la internet a través de tu teléfono inteligente sobre conexiones móviles de datos o WiFi puede ofrecer muchas opciones para comunicarte de forma segura con las personas, utilizando por ejemplo *VoIP* [12] e implementando medios para asegurar este canal de comunicación. Incluso, algunos teléfonos inteligentes pueden extender la seguridad a llamadas de teléfono móvil, más allá de VoIP (Ver **Redphone** abajo).

Aquí enumeramos algunas herramientas, con sus pros y contras:

Skype

La aplicación comercial VoIP más popular *Skype* [13] está disponible para todas las plataformas de teléfonos inteligentes y funciona si tu conexión inalámbrica es fiable. Es menos seguro en conexiones de data móvil.

En la ***Sección 3*** [14] del ***Capítulo 7: Mantener privada tu comunicación en Internet*** [14], conversamos sobre los riesgos al utilizar Skype, y porqué, si es posible, debemos evitar usuarlo. En resumen, Skype no es un software de Código Abierto lo que dificulta verificar de forma independiente sus niveles de seguridad. Adicionalmente, Skype es propiedad de Microsoft, el cual tiene el interés comercial de saber cuándo utilizas Skype y desde dónde. Así mismo, Skype podría permitirle a las agencias de la fuerza del orden acceso retrospectivo de todo tu historial de comunicaciones.

Otros VoIP

Utilizar VoIP generalmente es gratuito (o significativamente más barato que las llamadas

móviles) y deja menos rastros de tus datos. Es más, una llamada segura con VoIP puede ser la forma más segura de comunicarse.

CSipSimple [15] es un poderoso cliente VoIP para teléfonos Android, que cuenta con excelente mantenimiento y contiene sencillas configuraciones de asistente para diferentes servicios VoIP.

Open Secure Telephony Network (OSTN) [16] y el servidor de Guardian project, **ostel.me** [17], actualmente ofrece uno de los medios más seguros para la comunicación de voz. Conocer y confiar en el proveedor que opera el servidor de tu comunicación VoIP es de vital importancia. Los que hospedan este servicio – **Guardian Project** [18] – son bien conocidos y respetados en la comunidad.

Al utilizar CSipSimple, nunca te comunicas directamente con la otra persona, en vez de ello todos tus datos se canalizan a través del servidor Ostel. Esto hace que sea mucho más difícil rastrear tus datos y averiguar con quién te estás hablando. Adicionalmente, Ostel no guarda ninguna información, excepto los datos de la cuenta que necesitas para iniciar la sesión. Todas tus conversaciones están cifradas; y tus meta datos (los cuales son usualmente muy difíciles de ocultar) son borrosas porque el tráfico pasa por el servidor ostel.me. Si descargas CSipSimple desde ostel.me, ya vendrá configurado para utilizarlo con ostel.me lo que lo hace aún más fácil de instalar y usar.

RedPhone [19] es una aplicación gratuita y Código Abierto que cifra datos de comunicación de voz enviados entre dos dispositivos que corren con esta misma aplicación. Es fácil de instalar y fácil de utilizar, ya que se integra a tu marcado normal y sistema de contactos. Sin embargo las personas con las que deseas comunicarte también necesitan instalar y utilizar RedPhone. Para facilitar el uso RedPhone utiliza su número de teléfono móvil como su identificador (como un nombre de usuario en otros servicios VoIP). Sin embargo, se vuelve más sencillo analizar el tráfico que produce y rastrearte de vuelta a través de tu número de teléfono móvil. RedPhone utiliza un servidor central como punto de centralización pone a RedPhone en una poderosa posición (por tener control sobre algunos esto datos).

Estamos desarrollando las Guías Prácticas para CSipSimple, Ostel.me y Redphone. Por el momento, puedes encontrar más información en los enlaces disponibles arriba.

Enviando Mensajes de forma Segura

Debes tomar precauciones a la hora de enviar SMS o al utilizar mensajería instantánea o chat en tu teléfono inteligente.

SMS

Como se describe en el ***Capítulo 10.2.3 Comunicaciones textuales – SMS / Mensajes de Texto*** [20], la comunicación SMS es insegura por defecto. Cualquier persona con acceso a una red de telecomunicación móvil puede interceptar fácilmente los mensajes, y esto es una acción cotidiana que se da en muchas situaciones. No se confíe enviando mensajes SMS inseguros en situaciones críticas. No existen ninguna forma de autenticar un mensaje SMS, por lo tanto es imposible saber si el contenido de dicho mensaje fue alterado durante su envío o si el emisor del mensaje realmente es la persona que dice ser.

Asegurando los SMS

TextSecure [21] es una herramienta de Código Abierto *FOSS* [8] para enviar y recibir SMS de forma segura en los teléfonos Android. Funciona tanto para mensajes cifrados y no cifrados, así que puedes utilizarla por defecto como una aplicación SMS. Para intercambiar mensajes cifrados esta herramienta debe estar instalado tanto por parte del emisor como del receptor del mensaje, por lo tanto deberás promover su uso constante entre las personas con las que te comunicas. TextSecure automáticamente detecta los mensajes cifrados recibidos desde otro usuario de TextSecure. También te permite cifrar mensajes a más de una persona. Los mensajes son firmados automáticamente haciendo casi imposible que los contenidos del mensaje sean alterados. En nuestras guía sobre TextSecure explicamos en detalle las características de esta herramienta y cómo utilizarla.

Guía Práctica: Empezar con la *Guía de TextSecure* [22]

Chat Seguro

La mensajería instantánea o chat en tu teléfono puede producir mucha información vulnerable a la interceptación. Estas conversaciones podrían ser usadas en tu contra por adversarios posteriormente. Deberías por lo tanto ser extremadamente cauteloso/a sobre lo que escribes en tu teléfono mientras envías mensajes instantáneos y al chatear.

Existen formas seguras para chatear y enviar mensajes instantáneos. La mejor forma es utilizar cifrado de extremo a extremo (doble vía), asegurando que la persona al otro extremo sea la persona con la que deseas comunicarte.

Recomendamos **Gibberbot** [23] por ser una aplicación segura para chatear en teléfonos Android. Gibberbot ofrece cifrado sencillo y fuerte para tus chats con el protocolo de mensajería *Off-the-Record* [24]. Este cifrado provee ambas autentificaciones, por un lado puedes verificar que chateas con la persona correcta, y por otro lado contiene seguridad independiente entre cada sesión, de esta forma si una sesión de chat cifrado se ve comprometida, otras sesiones pasadas o futuras se mantendrán seguras.

Gibberbot ha sido diseñado para funcionar en conjunto con Orbot, de esta forma tus mensajes de chat son canalizados a través de la red anónima *Tor* [25]. Esto hace que sea muy difícil de rastrear o incluso averiguar si sucedió alguna vez.

Guía Práctica: Empezar con *Gibberbot Guide* [26]

Para clientes de iPhones, el **ChatSecure** [27] provee las mismas características, sin embargo no es tan sencillo utilizarlo con la red de *Tor* [28].

Estamos desarrollando las Guías Prácticas para ChatSecure. Por el momento, puedes encontrar más información en homepage [27].

Independientemente de la aplicación que utilices, siempre considera desde cuál cuenta usarás el chat. Por ejemplo, cuando utilizas Google Talk, tus credenciales y tiempo de la sesión del chat serán conocidas por Google. Ponte de acuerdo con tus contactos para no dejar guardados los historiales de chat, especialmente si no están cifrados.

Guardando Información en tu Teléfono Inteligente

Los teléfonos inteligentes vienen con gran capacidad de almacenamiento de datos. Desafortunadamente, los datos guardados en tu dispositivo pueden ser fácilmente accesibles a terceras personas, ya sea de forma remota o con acceso físico al teléfono. Algunas precauciones básicas sobre cómo reducir el acceso indebido a esta información se explica en la ***Guía de Configuración Básica para Android*** [6]. Adicionalmente, puedes tomar medidas para cifrar información sensible en tu teléfono utilizando herramientas específicas.

Herramientas para cifrar datos

El **Android Privacy Guard (APG)** [29] permite cifrar archivos y correos electrónicos con OpenGPG. También puede ser usado para mantener tus archivos y documentos seguros en tu teléfono, así como cuando envías correos electrónicos.

Guía Práctica: Empezar con *APG Guide* [29]

El **Cryptonite** [30] es otra herramienta de Código Abierto *FOSS* [8] para cifrar archivos. Cryptonite tiene características más avanzadas para teléfonos Android especialmente preparados con firmware personalizado. Para más información, ver la sección ***Uso Avanzado de Teléfonos Inteligentes*** [31].

Guía Práctica: Empezar con *Cryptonite Guide* [32]

Manejo de Contraseñas Seguras

Puedes mantener todas tus contraseñas un solo lugar archivo cifrado de forma segura utilizando **Keepass**. Sólo deberás recordar una clave o contraseña maestra para acceder a todas las otras contraseñas. Con Keepass puedes usar contraseñas muy fuertes para cada una de tus cuentas, ya que Keepass las recordará para tí, además viene con un generador automático de contraseñas para crear contraseñas nuevas. Puedes sincronizar la base de datos de Keepass entre tu teléfono y tu computadora. Te recomendamos sincronizar sólo aquellas contraseñas que usas cotidianamente en tu teléfono móvil. Puedes crear y separar en pequeñas bases de datos las contraseñas en la computadora, y posteriormente sincronizar una a tu teléfono móvil en lugar de copiar la base de datos entera de todas tus contraseñas. Como todas tus contraseñas estarán protegidas por una contraseña maestra, es de vital importancia que esta contraseña sea muy fuerte para proteger tu base de datos de Keepass. Ver ***Capítulo 3: Crear y mantener contraseñas seguras*** [33].

Guía Práctica: Empezar con la *Mini Guia de Keepass* [34]

Enviando Correos Electrónicos con Teléfonos Inteligentes

En esta sección abordaremos brevemente el uso de correo electrónico con teléfonos

inteligentes. Te instamos a revisar las secciones ***Asegurar tu correo electrónico*** [35] y ***Consejos para responder ante una sospecha de vigilancia de correo electrónico*** [36] en el ***Capítulo 7: Mantener privada tu comunicación en Internet*** [37] en las que conversamos sobre la seguridad básica del correo electrónico.

En primera instancia, considere si realmente necesitas acceder a tu correo electrónico con tu teléfono inteligente. Asegurar una computadora y su contenido, generalmente es más sencillo que hacerlo con un dispositivo móvil como el teléfono inteligente. Un teléfono inteligente es más suceptible a robos, vigilancia e intrusiones.

Si es absolutamente necesario acceder a tu correo electrónico a través de tu teléfono inteligente, existen acciones que puedes implementar para aminorar los riesgos:

- No consideres tu teléfono inteligente como el principal medio para acceder a tu correo electrónico. Descargar (y eliminar) correos electrónicos de un servidor de correos y guardarlos sólo en tu teléfono inteligente no es recomendable. Puedes configurar tu aplicación de correo electrónico para usar únicamente las copias de tus correos.

- Si utilizas correo cifrado con tus contactos, considere la instalación del mismo en tu teléfono móvil también. El beneficio adicional es que los correos cifrados permanecerán secretos si el teléfono cae en las manos equivocadas.

Guardar tu llave privada de cifrado en tu teléfono móvil puede parecer un riesgo. Sin embargo, el beneficio de poder enviar y guardar tus correos electrónicos cifrados y seguros en el dispositivo móvil pesa más que el riesgo. Considera generar un par de llaves únicas de cifrado para móvil (usando **APG** [38]) en tu teléfono inteligente, de esta forma evitas copiar tu llave privada de tu computadora al dispositivo móvil. Nota que esto requiere preguntarle a las personas con las que te comunicas, que también deben cifren sus correos electrónicos utilizando la llave única de cifrado de móviles.

Guía Práctica: Empezar con la *Guía sobre K9 y APG* [39]

Capturando Multimedias con Teléfonos Inteligentes

Capturar fotos, videos o audios con tu teléfono inteligente puede ser un medio poderoso para documentar y compartir eventos importantes. Sin embargo, es importante ser cuidadoso/a y respetuoso/a de la privacidad y seguridad de las personas fotografiadas, filmadas o grabadas. Por ejemplo, si tomas fotos o filmas y grabas un evento importante, puede ser peligroso para tí o para los que aparecen en las grabaciones si tu teléfono cae en las manos equivocadas. En estos casos, estas sugerencias pueden ser de ayuda:

- Ten un mecanismo de seguridad para subir los archivos multimedia en un lugar protegido en internet, y elimínalos del teléfono inmediatamente (tan pronto le sea posible).

- Usa herramientas para difuminar rostros de las personas que aparecen en las imágenes o videos, o distorsiona las voces de los audio y grabaciones de video, y sólo guarde las copias distorsionadas y difuminadas en archivos multimedia en tu dispositivo móvil.

- Proteja o remueva la meta información relacionada con tiempo y lugares dentro que quedan registrados en los archivos multimedia.

El **Guardian Project** [18] ha creado una aplicación de Código Abierto *FOSS* [8] llamada **ObscuraCam** [40] que identifica los rostros en las fotos y los difumina. Por supuesto que puedes escoger el modo de difuminación y qué deseas difuminar. Obscuracam también elimina las fotos originales, y si tienes un servidor para subir los multimedia grabados, provee funciones fáciles para subirlos.

Guía Práctica: Empezar con la *Guía de Obscuracam* [41]

En este momento, la organización de derechos humanos **Witness** [42] está trabajando con el Guardian project en una solución para los tres puntos expuestos anteriormente.

Acceso a Internet Seguro con Teléfonos Inteligentes

Según se abordó en el ***Capítulo 7: Mantener privada tu comunicación en Internet*** [37] y en el ***Capítulo 8: Mantenerse en el anonimato y evadir la censura en Internet*** [43], acceder a contenidos en Internet, o publicar fotos y videos, dejan huellas y rastros de quién eres y dónde estás y qué estás haciendo. Esto puede ponerte en riesgo. Utilizar tu teléfono inteligente para comunicarte con la internet aumenta considerablemente estos riesgos.

Acceso mediante WiFi o Data Móvil

Los teléfonos móviles te permiten controlar cómo accedes a Internet: vía conexión inalámbrica desde un punto de acceso (como un internet café o cyber), o vía conexión de data móvil, tales como GPRS, EDGE, o UMTS que ofrece tu proveedor de red móvil.

Utilizar una conexión WiFi reduce los rastros o huellas de los datos que estás dejando en tu proveedor de servicios de telefonía móvil (ya que no estás conectado/a con tu suscripción de teléfono móvil). A pesar de ello, algunas veces la conexión de data móvil es la única forma de estar en línea. Desafortunadamente, los protocolos de la conexión de data móvil (como EDGE o UMTS) no tienen protocolos abiertos. Desarrolladores independientes e ingenieros de seguridad no pueden examinar estos protocolos para ver cómo están siendo implementados por operadores de data móvil.

En algunos países los proveedores de servicios móviles operan bajo diferentes legislaciones que los proveedores de servicios de internet, lo que puede resultar en una mayor vigilancia por parte de gobiernos y responsables del soporte.

Independientemente del camino que tomes para tus comunicaciones digitales con teléfonos inteligentes, puedes reducir los riesgos de exponer datos mediante el uso de herramientas para el cifrado y anonimato.

Anonimizar

Para acceder a contenido en línea de forma anónima, puedes usar la aplicación para Android

llamada **Orbot** [44]. Orbot canaliza tu comunicación en internet mediante la red anónima de Tor.

Guía Práctica: Empezar con la *Guía de Orbot* [45]

Otra aplicación llamada Orweb, tiene la característica de ser un navegador web con potentes características de privacidad utilizando proxies que no guardan el historial de la navegación local. Juntos Orbot y Orweb eluden los filtros y cortafuegos en la web, y ofrecen navegación anónima.

Guía Práctica: Empezar con la *Guía de Orweb* [46]

Proxies

La versión móvil del navegador *Firefox* [47] – **Firefox mobile** [48] puede equiparse con complementos proxy que dirigirán tu tráfico a un servidor proxy. Por lo tanto, tu tráfico irá al sitio que estás solicitando. Esto es poderoso en casos de censura, pero puede que revele tus solicitudes si tu conexión desde tu cliente al proxy no está cifrada. Recomendamos el complemento llamado **Proxy Mobile** [49] (también de el **Guardian Project** [50], el cual hace que el proxy con Firefox sea sencillo. Así mismo, es la única forma de canalizar la comunicación móvil de Firefox a Orbot y utilizar la red *Tor* [28].

Seguridad Avanzada para Teléfonos Inteligentes

Obtén acceso completo a tu teléfono inteligente

La mayoría de los teléfonos inteligentes son capaces de hacer más que lo que ofrece el sistema operativo instalado en ellos, del software manufacturado (firmware) o de los programas del operador móvil. Al contrario, algunas funcionalidades están "encerradas" por lo que el usuario no es capaz de controlar o alterar estas funciones, y están fuera de alcance. En la mayoría de casos, esas funcionalidades son innecesarias para los usuarios de teléfonos inteligentes. Sin embargo, existen algunas aplicaciones y funcionalidades que pueden aumentar la seguridad de datos y comunicaciones en el teléfono inteligente. También existen otras funciones existentes que se pueden remover para evitar riesgos a la seguridad.

Por esto, y por otras razones, algunos usuarios de teléfonos inteligentes prefieren manipular los diversos programas y software ya instalados en los teléfonos inteligentes con el fin de obtener privilegios que les permite instalar funciones mejoradas, o remover y/o reducir otras.

El proceso de superar los límites impuestos por el operador móvil, o manufactureros de los sistemas operativos en un teléfono inteligente se llaman “rooting” (en el caso de dispositivos de Android), o “jailbreaking” (en el caso de dispositivos iOS como iPhone o iPad). Normalmente, el éxito del “rooting” o “jailbreaking” tiene como resultado obtener todos los privilegios necesarios para instalar o utilizar aplicaciones adicionales, realizar modificaciones a configuraciones bloqueadas, y control total sobre los datos guardados y la memoria del teléfono inteligente.

ADVERTENCIA: El "rooting" o "jailbreaking" no es un proceso reversible, y requiere de experiencia en la instalación y configuración de software. Considere lo siguiente:

- Existe el riesgo de que tu teléfono inteligente quede permanentemente inoperable, o "bricking it" (eje convertirlo en un ladrillo).
- La garantía del manufacturero u operador móvil puede quedar sin efecto o anulada.
- En algunos lugares este proceso puede ser considerado ilegal.

Pero si eres cuidadoso/a, un dispositivo "rooted" puede ser una forma sencilla de obtener mayor control sobre los teléfonos inteligentes hacerlo mucho más seguro.

Firmware Alternativo

Firmware se refiere a programas que están estrechamente relacionados a un dispositivo en particular. Están en cooperación con el sistema operativo del dispositivo y son responsables de la operación básica del hardware de tu teléfono inteligente, tales como el micrófono, parlantes, cámara, pantalla táctil, memoria, llaves, antenas, etc.

Si tienes un dispositivo Android, puedes considerar instalarle un firmware alternativo para mejorar aún más tu control sobre el teléfono. Nota que para instalar firmware alternativo implementa el proceso de "rooting" a tu teléfono.

Un ejemplo de un firmware alternativo para un teléfono Android es **Cyanogenmod** [51], el cual te permite desinstalar aplicaciones al nivel del sistema de tu teléfono (eje, aquellas aplicaciones instaladas por el manufacturero del teléfono o tu operador de red móvil). Al hacerlo, puedes reducir la cantidad de formas en las que tu dispositivo es monitoreado, como cuando la información es enviada a tu proveedor de servicios sin tu conocimiento.

Adicionalmente, Cyanogenmod navega por defecto con una aplicación OpenVPN (RPV por sus siglas en español), que en caso contrario sería tedioso instalar. RPV (Red Privada Virtual, siglas en inglés) es una de las formas de asegurar el proxy de tu comunicación en internet (ver abajo).

Cyanogenmod también ofrece un modo de navegación Incógnito en el cual el historial de tus comunicaciones no es registrada en tu teléfono inteligente.

Cyanogenmod viene con muchas otras características. Sin embargo, no es compatible con todos los dispositivos de Android, así que antes de continuar revisa la lista de dispositivos compatibles [52].

Cifrar volúmenes completos

Si tu teléfono ha sido "rooted" quizá quieras cifrar todo el espacio de almacenamiento de datos, o bien crear un volumen en el teléfono inteligente para proteger alguna información en el teléfono.

Luks Manager [53] le permite cifrar volúmenes con alta seguridad y de forma instantánea mediante una interfaz amigable. Es altamente recomendable que instale esta herramienta antes de empezar a guardar datos en tu dispositivo Android y utilizar los Volúmenes Cifrados que provee el Luks Manager para almacenar tus datos.

El proyecto Whisper Systems está preparando un aplicación llamada **WhisperCore** [54] que te permitirá un cifrado total de tu dispositivo Android.

Red Privada Virtual (RPV)

Una RPV ofrece un túnel cifrado a través de la internet entre tu dispositivo y un servidor RPV. Esto se llama un túnel porque a diferencia de otros tráficos cifrados, como https, esconde todos los servicios, protocolos y contenidos. Una conexión RPV se configura una sola vez, y termina solo cuando tu lo decidas.

Ten en cuenta que como todo tu tráfico viaja a través de un servidor proxy o RPV, un intermediario sólo necesitará acceso al proxy para analizar tus actividades. Por lo tanto, es sumamente importante que escojas cuidadosamente entre los servicios de proxy y de RPV. También es recomendable utilizar diferentes proxys y/o RPV, ya que al distribuir en diferentes canales tus datos se reduce el impacto de un servicio en peligro.

Recomendamos el uso del servidor **RiseUp VPN** [55]. Puedes utilizar RiseUp VPN en un dispositivo Android después de instalar Cyanogenmod (ver arriba). Además es muy fácil de configurar la conexión del RiseUp VPN a un iPhone – para más información leer aquí [56].

Enlaces:
[1] https://securityinabox.org/es/chapter-10
[2] https://securityinabox.org/en/Glossary#GPS
[3] https://securityinabox.org/es/chapter-5
[4] https://securityinabox.org/es/Glossary#FOSS
[5] https://securityinabox.org/es/glossary#GPS
[6] https://securityinabox.org/en/android_basic
[7] http://f-droid.org
[8] https://securityinabox.org/en/glossary#FOSS
[9] https://securityinabox.org/en/glossary#apk
[10] https://securityinabox.org/es/chapter_10_2
[11] https://securityinabox.org/es/chapter_10_2_2
[12] https://securityinabox.org/en/Glossary#VoIP
[13] https://securityinabox.org/en/glossary#skype
[14] https://securityinabox.org/es/chapter_7_3
[15] http://f-droid.org/repository/browse/?fdid=com.csipsimple&fdpage=4
[16] https://guardianproject.info/wiki/OSTN
[17] https://ostel.me
[18] https://guardianproject.info
[19] https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
[20] https://securityinabox.org/es/chapter_10_2_3
[21] https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
[22] https://securityinabox.org/es/textsecure_principal
[23] https://guardianproject.info/apps/gibber/
[24] https://securityinabox.org/en/glossary#OTR
[25] https://securityinabox.org/es/glossary#Tor
[26] https://securityinabox.org/es/gibberbot_principal
[27] https://chatsecure.org
[28] https://securityinabox.org/en/glossary#Tor
[29] https://securityinabox.org/en/apg_main
[30] https://code.google.com/p/cryptonite/
[31] https://securityinabox.org/es/chapter_11_7
[32] https://securityinabox.org/en/Cryptonite_main
[33] https://securityinabox.org/es/chapter-3

[34] https://securityinabox.org/en/keepassdroid_main
[35] https://securityinabox.org/es/chapter_7_1
[36] https://securityinabox.org/es/chapter_7_2
[37] https://securityinabox.org/es/chapter-7
[38] https://securityinabox.org/es/APG_principal
[39] https://securityinabox.org/es/K9_APG_principal
[40] https://guardianproject.info/apps/obscuracam/
[41] https://securityinabox.org/es/Obscuracam_principal
[42] https://www.witness.org
[43] https://securityinabox.org/es/chapter-8
[44] https://www.torproject.org/docs/android.html.en
[45] https://securityinabox.org/es/Orbot_principal
[46] https://securityinabox.org/es/Orweb_principal
[47] https://securityinabox.org/en/glossary#Firefox
[48] http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox
[49] https://guardianproject.info/apps/proxymob-firefox-add-on/
[50] https://guardianproject.info/
[51] http://www.cyanogenmod.com
[52] http://www.cyanogenmod.com/devices
[53] http://www.whispersys.com/
[54] http://www.whispersys.com/whispercore.html
[55] https://help.riseup.net/en/vpn
[56] https://support.apple.com/kb/HT1424